MARITIME DOMAIN AWARENESS

Myths and Realities

Commander Steven C. Boraz, U.S. Navy

Maritime Domain Awareness is where it all begins. We cannot conduct the operations that we must if we don't have a good sense of what's out there, moving on, above or under the sea.

ADMIRAL GARY ROUGHEAD, IN *RHUMB LINES,* 20 AUGUST 2007

It was not long after the attacks of September 11th that government officials began discussing other avenues that terrorists might use to attack American citizens, particularly in the maritime domain. In a speech delivered in January 2002, President George W. Bush noted, "The heart of the Maritime Domain Awareness program is accurate information, intelligence, surveillance, and reconnaissance of all vessels, cargo, and people extending well beyond our traditional maritime boundaries."[1] By November 2002 Congress had passed the Maritime Transportation Security Act of 2002.[2] The National Security Council and the president continued to explore issues surrounding the safety and security of the U.S. maritime environs. In December 2004, the president signed National Security Presidential Directive 41/Homeland Security Presidential Directive 13, which established policy guidelines. It also directed the secretaries of Homeland Security and Defense to lead the federal effort in developing a comprehensive national strategy that would better integrate and synchronize existing department-level strategies and ensure their effective and efficient implementation. The interagency Maritime Security Policy Coordinating Committee was established to serve as the primary forum for coordinating government maritime security policies; it delivered a National Strategy for Maritime Security in September 2005.[3] Eight additional plans, including the National Plan to Achieve Maritime Domain Awareness, buttress the national strategy.[4]

Commander Boraz, an eighteen-year veteran of the U.S. Navy's intelligence community, is currently the Assistant Program Manager for Maritime Domain Awareness at Program Executive Office, Command, Control, Communications, Computers, and Intelligence in San Diego, California. He served as a Federal Executive Fellow at the RAND Corporation from 2004 to 2005. He has published in several professional journals and is coeditor of Reforming Intelligence: Obstacles to Democratic Control and Effectiveness (Austin: University of Texas Press, 2007).

Naval War College Review, Summer 2009, Vol. 62, No. 3

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Maritime Domain Awareness: Myths and Realities	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval War College,686 Cushing Road,Newport,RI,02841-1207**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**10**	

In response, the departments of Homeland Security, Transportation, and Defense identified executive agents to lead their efforts toward achieving maritime domain awareness (MDA): the Coast Guard, the Maritime Administration, and the Navy, respectively.

The Coast Guard has recently established the Nationwide Automatic Identification System, a robust command-and-control network designed to improve maritime safety and security at the nation's highest-priority ports and coastal zones. Customs and Border Protection, another Homeland Security agency, has the Container Security Initiative and the Customs-Trade Partnership against Terrorism (C-TPAT).[5]

The Maritime Administration helped develop the Maritime Safety and Security Information System (MSSIS), participates in the MDA executive steering committee, and is tasked by Congress to be the "Information Advocate of the Marine Transportation System."[6]

The Navy, for its part, has pushed the concept of the "thousand-ship navy";[7] at least one senior advocate has declared that "it is virtually indisputable that MDA is the enabling mission supporting Sea Strike, Sea Shield, and Sea Basing, and is a primary focus of what FORCEnet will ultimately do."[8] MDA is a key component in the Navy's new maritime strategy, *A Cooperative Strategy for 21st Century Seapower,* which notes, "To be effective, there must be a significantly increased commitment to advance *maritime domain awareness* (MDA). . . . Maritime forces will contribute to enhance information sharing, underpinning and energizing our capability to neutralize threats to our Nation as far from our shores as possible."[9]

The Secretary of the Navy has deemed MDA important enough to direct the service to develop a "cross-functional team" from the operational staff and acquisition communities to implement an initial MDA capability in the Central and Pacific Command areas of responsibility and on the west coast of the United States by August 2008; the secretary committed more than $300 million to doing so.[10] There are literally hundreds more public and commercial MDA-related activities being developed.

MDA is also a contemporary debate topic. This journal, for example, has provided ample space to the maritime strategy and MDA, and it routinely publishes articles regarding maritime security.[11] Also, maritime security figures prominently in literature issued by think tanks.[12]

Even without such extensive and varied activity, it would be clear that MDA is a cornerstone of national security, as more than 80 percent of the world's trade travels by water.[13] Nonetheless, operators, acquisition professionals, defense contractors, and policy makers still find maritime domain awareness a difficult idea. This is the case because of widespread misperceptions about what it takes

to achieve MDA, who should implement it, where, and how. This article is intended to address and clear away some of those stumbling blocks.

Myth: "The Navy Has Always 'Done' MDA"

The reality is that navies of the world, both ancient and modern, have always gathered data on their maritime environments to gain situational awareness that their missions required, whether basic navigation or finding an enemy armada and stopping it before it could attack. Many argue that there has simply been a change in the details; in fact, however, that would be akin to saying humanity had been "doing" physics before Isaac Newton—the context of the MDA we've been "doing" and that of the MDA we need to achieve are vastly different. This is true for three reasons.

First, the scale of "doing" MDA has dramatically expanded; massive amounts of data on all aspects of maritime activity must be collected, then cross-referenced, "fused" (generally speaking, correlated across sources), and analyzed, in order to detect anomalies that may indicate threat-related behavior.[14] The computing power required is inordinately greater than the capacity of the "grey matter" of those keeping watch. For example, during the Cold War probably fewer than a thousand ships were tracked globally at any one time. Today, hundreds of thousands of ships need to be tracked *and* the links among their cargoes, crews, and financial transactions sorted out. The November 2008 seaborne attacks on Mumbai represent a vivid case in point. The attackers hijacked an Indian fishing trawler, the *Kuber,* which routinely traveled to Mumbai from a port in Gujarat State near the India-Pakistan border. Approximately 950 trawlers, carrying eight thousand fishermen, come to Mumbai every year, over an eight-month period beginning in August.[15] Making the connections between these trawlers and the terrorists who may take advantage of such logistics networks requires much more than "what we've always been doing."

Second, the U.S. Navy has let the arts of understanding regional maritime activity and determining trends therein atrophy. For years, this was a mission assigned to Fleet Ocean Surveillance Information Facilities and Centers (FOSIFs and FOSICs). Staffed with naval intelligence professionals, "operators," and civilian analysts, they provided in-depth analysis of the activities of the navies (and some air forces) in all the maritime environs in which the U.S. Navy operated.[16] In the restructuring that resulted from the demise of the Soviet Union and a new U.S. emphasis on joint structures, the missions that FOSIFs and FOSICs had once met were transferred to Joint Intelligence Centers (JICs). Whether because the maritime environment has changed so drastically—that is, no Soviet navy—or because, as some contend, the centers simply ignore maritime issues and focus their intelligence support on combatant commanders (i.e.,

of unified, or interservice, regional or functional commands) rather than operational forces, is immaterial. The result is less support to naval forces. The emerging "Maritime Headquarters with Maritime Operations Centers" (MHQ/MOC) concept may fill the gap. MHQ/MOC envisions a global network of Navy-maritime organizations in support of national requirements.[17] The initial plan establishes MHQs for each of the "numbered fleets" (e.g., the Seventh Fleet in the western Pacific Ocean, the Sixth Fleet in the Mediterranean, etc.). A "concept of operations" argues:

> A key element of both homeland defense and maritime security overseas is achieving and maintaining global maritime intelligence integration (GMII) and maritime domain awareness (MDA), which will require integrating various local and regional estimates within a global context. Maritime forces are a key element in this layered defense of national interests, both in the forward regions and in the approaches to the continental United States, where the objective is "to detect, deter, and, if necessary, defeat threats en route—before they reach the United States."[18]

Applied regional MDA expertise, then, is urgently needed. Imagine, in a war-fighting context, having to determine the intention of a particular merchant ship for the commander of the Seventh Fleet, or of the entire Pacific Fleet, and "turning on the MDA switch" to do so—only to find the circuit not connected. When the Soviet navy was at sea, teams kept checklists on its specific activities, past and present; they knew what each one meant and had a very good idea as to what would follow. Today, in contrast, the U.S. Navy does not have the intelligence, operational, intellectual, or technical capacity to support MDA-related missions at the operational level of war. Part of the shortfall is being addressed by new programs, as well as by the reestablishment of the Advanced Maritime Operational Intelligence Course at the Center for Naval Intelligence in Dam Neck, Virginia, but these very initiatives are evidence that the gap exists.

Third, the way the Navy views commercial merchant traffic (traditionally color coded as "white") has changed. White shipping used to be a navigational and watch-keeping problem—something not to collide with or at which not to direct missiles. Now it is a potential threat as evinced by the al-Qa'ida attacks on the USS *Cole* in 2000 and the crude-oil carrier M/V *Limburg* in 2002, the Mumbai attacks, and numerous acts of piracy off the Horn of Africa, in the Malacca Strait, and elsewhere.

Myth: "MDA Is All about 'White' Shipping"

In reality, maritime domain awareness is about considerably more than white shipping. As we have seen, it puts white shipping in an entirely different light; however, MDA is "the effective understanding of anything associated with the

global maritime domain that could impact the *security, safety, economy, or environment* of the United States."[19] Maritime domain awareness means finding the ships and submarines of friends and foes, understanding the entire supply chain of cargoes, identifying people aboard vessels, understanding the infrastructures within or astride the maritime domain, and identifying anomalies and potential threats in all these areas. Naval officers, however, focus more often than not on security aspects; for them, MDA boils down to a maritime targeting issue. "Targeting," in this sense, does not always involve a "kinetic effect" (a weapon striking an object). It may mean pointing out to a boarding team a merchant vessel that it should strike up a conversation with; identifying a cargo carrier as suspect so it can be held offshore for inspection; understanding the flows of personnel and cargo at a shore facility; or, when a kinetic targeting solution is required, picking out the wheat from the chaff.

Myth: "MDA Is Too Amorphous a Concept to Be Useful"

In reality—and while maritime domain awareness certainly has different meanings for Captains of Ports, masters of ships, and everyone in between—the common requirements of safety, security, the economy, and the environment resonate among all its stakeholders. This was evident at the MDA Connectivity Workshop conference held in Newport, Rhode Island, in August 2007 and attended by representatives of Australia, Canada, France, Italy, Japan, NATO, New Zealand, Singapore, the United Kingdom, and the United States. The international attendees agreed that "maritime domain awareness" was a flawed rubric and that implied links to the U.S. global war on terror were worrisome. But their primary maritime-security concerns were surprisingly similar: terrorism, illegal migration, piracy, illegal exploitation of natural resources, illegal activity in protected areas, drug trafficking, arms smuggling, and the need for security and environmental protection. That is, admittedly, a broad range of issues, but the fact that so many disparate nations share them testifies to the importance of maritime domain awareness and the prospects for partnerships to achieve it.

Myth: "MDA Is All about the Blips on My Monitor"

The reality is that MDA is not just about the blips; it's about whether the blips matter. Aggregating disparate data sets to generate a useful operational picture is an increasingly complex task because of the massive amounts of data available on all aspects of maritime activity. Fusing and analyzing those data may find anomalies that point to threat activity of interest to decision makers. The Navy's formal MDA concept lays it out as an equation: that maritime domain awareness equals global maritime situational awareness (the blips) plus maritime threat awareness (whether the blips matter).[20]

Myth: "All We Need for MDA Is AIS"

The Automatic Identification System, or AIS, is indeed a reality. It uses a signal—a transponder-based collision-avoidance system that transmits and receives real-time navigational information via VHF line-of-sight radio—that can be shared freely at the unclassified level. The International Maritime Organization (IMO) mandates its use on all passenger ships, tankers, and all other ships of three hundred gross tons and above.[21] AIS is a critical technology that enables MDA. Its use has spawned navigational information networks and "clearinghouses" in many nations; it is a key component of MSSIS; and it is available commercially.[22]

However, the Automatic Identification System has its weaknesses. It can be spoofed, its use is loosely enforced (if at all), and it provides information only on ships mandated by the IMO; potential foes know how to use it, or not use it, so as to hide their whereabouts. Moreover, due to the nature of the underlying communications protocol (known as "time-division multiplexing") that AIS employs, signal degradation in high-density environments limits the usefulness of the system as well as the value of its proposed use on smaller ships. Strategic partners have produced technical solutions that overcome this liability, by means of the Global Packet Radio Service, a system in use for many mobile phones.

The underlying issue is that neither AIS nor any other "silver bullet" will achieve maritime domain awareness. MDA requires all manner of sensors, databases, data sharing, decision aids, displays, etc. Without databases that can be rapidly and adaptively searched to develop trends on specific ships, AIS does little more than "spam" the maritime "common operational picture" with more and more blips.

Myth: "MDA Can Be Done Entirely at the Unclassified Level"

The reality is that our ability to find, fix, track, and target is considerably enhanced when classified or sensitive information is applied. There is no doubt that much of the information available to achieve maritime domain awareness is unclassified. Programs like the Container Security Initiative, C-TPAT, MSSIS, and of course AIS have been of considerable benefit to safety and security in the maritime domain. But how often will operational decisions be made on the basis of what is essentially a navigational-hazard and ship-avoidance system? As Vice Admiral John Morgan and Commander Bud Wimmer point out, "Maritime Domain Awareness is all about generating actionable intelligence, the cornerstone of successful counterterrorist and maritime law enforcement operations."[23] While unclassified information can contribute significantly to "awareness" per se, producing

actionable intelligence generally requires classified or sensitive information not available in the public domain.

Myth: "We Can Just Build Something like ICAO for the Maritime Domain"

In reality, the maritime domain has unique compliance challenges, based on culture and competitive advantage. The International Civilian Aviation Organization (ICAO), a United Nations agency, codifies principles and techniques and sets standards to facilitate border crossing for international civil aviation.[24] According to some, the IMO should be able to do the same for the maritime environment.

ICAO standards are based on the Chicago Convention of 1945–47, a document that was agreed upon only two decades after the birth of international air travel and so influenced its formative years. To speak of something similar in the maritime domain fails to take into account that freedom of the seas has been a critical aspect of commercial trade and an international standard for well over two *millenniums*.

Moreover, commercial practice makes the analogy between the maritime and air domains a poor one. Airplanes file flight plans, take off, and land. Ships file sailing plans and depart but then, in a single extended voyage, may change flags, change owners, change names, sell cargo, change their destinations, all in an attempt to make, or not lose, money in a volatile, highly competitive shipping market, and while other ships are trying to do the same.

While the development of international standards for the maritime domain based on those now in effect for the air is a laudable goal and may be possible someday, those who argue for them tend to forget that cultural change takes time, usually proportionate to how long a culture has been in place. Further, the cost would likely meet with substantial resistance from many nations. Establishing ICAO-like standards in the maritime domain is simply not achievable in the near term.

Myth: "MDA Can Be Done Virtually"

The reality is that much of what the United States has learned since the terrorist attacks of 11 September 2001 points to the legal and cultural restrictions that hamper its ability to share information. There is little doubt that no single entity or agency can be responsible for, or has the capacity to coordinate, all MDA-related activity. That fact, coupled with modern network-centric information capabilities, leads to a strong argument that "nodes" generating maritime situational awareness must be linked and that some MDA functions must be done virtually. The present approaches that have worked best include those of the National Counterterrorism Center (in McLean, Virginia), the National Counterproliferation Center (in Washington, D.C.), and the Joint Interagency Task Forces (West

and South), because they put people and systems from different agencies into the same physical structures. This enables (in fact, forces) information sharing while ensuring that information does not cross information-security boundaries.

This brick-and-mortar solution might be applied to MDA in the form of what might be called "maritime interagency task forces." They would combine elements of MHQ/MOCs, numbered-fleet command centers, the U.S. Coast Guard's Maritime Intelligence Fusion Centers, and unified combatant commands and might initially be staffed by those entities. They would also need appropriate operations and intelligence specialists from various government agencies (some of them already in the combatant commands), selected allied nations, and commercial liaisons. The mission would be to deliver regionally focused expertise and operational support, for areas of responsibilities roughly coinciding with those of the numbered fleets.

This would require a hard look at existing structures both within and outside the continental United States, in particular the relationship among MHQ/MOCs, Joint Intelligence Operation Centers in each of the combatant commands, and Maritime Intelligence Fusion Centers. For instance, the maritime security mission of the Joint Intelligence Operation Center significantly overlaps that of the MHQ/MOC, especially overseas. Given today's resource constraints, combining people and missions is worth considering. The same can be said for centers within the United States itself, where the Coast Guard fusion centers would need to be accounted for as well.

Aside from the need for increased information sharing and better support to operational forces, new tactics, techniques, and procedures would naturally flow from these maritime interagency task forces. While technology will certainly help, increased maritime domain awareness is virtually meaningless without the tools needed by the decision makers who must carry out operational responses. This is a key point, one that cross-functional teams have repeatedly made.

To be sure, "federation" across maritime stakeholders (that is, a division of labor) will continue to be required. It is also of utmost import to get "reachback" capabilities right—the ability of deployed forces to call, very quickly, upon the full informational and analytical resources of intelligence commands back home. That reachback needs to be as responsive to fleets as the FOSICs and FOSIFs once were. Setting up regional "centers of maritime excellence" with the right people, equipment, and training would be a step in the right direction.

Maritime domain awareness is neither tracks on a screen, systems that monitor white shipping, (unachievable) international standards, nor something maritime security forces have always done. Nor is it easily achieved. But achieving maritime domain awareness is critically important in today's geopolitical context, not just to guard against international terrorism but to promote commerce

and safety and to respond to natural disasters, piracy, illegal migration, and arms smuggling.

MDA is an important part of this nation's security strategy, and achieving it will require new thinking regarding the roles of national and international maritime-security forces. Establishing "maritime interagency task forces," or something similar, will go a long way toward that goal. But whatever means it chooses, the United States is a maritime nation in a maritime world—achieving maritime domain awareness is a twenty-first-century strategic imperative.

NOTES

The views expressed here are those of the author and do not reflect the official policy or position of the Department of the Navy, the Department of Defense, or the U.S. government.

1. As quoted in U.S. Homeland Security Dept., *The National Plan to Achieve Maritime Domain Awareness* (Washington, D.C.: October 2005), available at www.dhs.gov/.
2. Public Law 107-295, 25 November 2002.
3. See *National Strategy for Maritime Security* (Washington, D.C.: White House, September 2005), available at www.whitehouse.gov/.
4. In addition to the National Plan to Achieve Maritime Domain Awareness, the supporting plans are the Global Maritime Intelligence Integration Plan, the Maritime Operational Threat Response Plan, the International Outreach and Coordination Strategy, the Maritime Infrastructure Recovery Plan, the Maritime Transportation System Security Plan, the Maritime Commerce Security Plan, and the Domestic Outreach Plan.
5. For more on the Container Security Initiative see "CSI Strategic Plan 2006–2011," *U.S. Customs and Border Protection,* www.cbp.gov/linkhandler/cgov/. For more on C-TPAT see "Securing the Global Supply Chain: C-TPAT Strategic Plan," *U.S. Customs and Border Protection,* www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/.
6. MSSIS collects and disseminates real-time data derived from the Automatic Identification System about vessel movements in the unclassified realm and is freely shared with international partners. At present, movements of more than ten thousand vessels from over forty nations are tracked and updated in real time. See "Volpe Center Highlights May/June 2006," *Volpe National Transportation Systems Center,* www.volpe.dot.gov/; and "Global Maritime Domain Awareness Wins Innovations in American Government Award," Reuters, 9 September 2008, available at www.reuters.com. For more on the Maritime Administration, see "MARAD Maritime Domain Awareness Point Paper," *Maritime Administration,* marad.dot.gov/documents/.
7. For more on the thousand-ship navy see Vice Adm. John G. Morgan, Jr., USN, and Rear Adm. Charles W. Martoglio, USN, "The 1,000 Ship Navy: Global Maritime Network" (November 2005), and "The Commanders Respond" (March 2006), both U.S. Naval Institute *Proceedings;* and Ronald E. Ratcliff, "Building Partners' Capacity: The Thousand-Ship Navy," *Naval War College Review* 60, no. 4 (Autumn 2007), pp. 45–58.
8. "Maritime Domain Awareness: A Global Maritime Security Mission Requiring International Cooperation and U.S. Navy Leadership," COMUSNAVEUR white paper, January 2006.
9. *A Cooperative Strategy for 21st Century Seapower,* October 2007, reprinted in *Naval War College Review* 61, no. 1 (Winter 2008), pp. 7–19; also available at www.navy.mil/maritime/MaritimeStrategy.pdf.
10. Secretary Winter directed these activities in a 17 May 2007 memorandum. The $300 million figure comes from several interviews with Mr. Marshall Billingslea, the secretary's

Deputy Under Secretary of the Navy. For example see Bettina Haymann Chavanne, "U.S. Navy Will Ask for $300m for Maritime Domain Awareness," *Aerospace Daily,* 10 September 2007; Geoff Fein, "Navy's MDA Effort to Provide Greater ID of Ocean-Going Threats," *Defense Daily,* 16 November 2007; and Zachary M. Peterson, "USN to Launch 'Actionable Intelligence' System," *Defense News,* 14 January 2008. This new capability was deemed "operational capable" in August of 2008, only fifteen months after the initial Secretary of the Navy memo. See Emelie Rutherford, "Navy's Maritime Domain Awareness System 'Up and Running,'" *Defense Daily,* 4 September 2008.

11. For example, see Geoffrey Till, "New Directions in Maritime Strategy? Implications for the U.S. Navy," vol. 60, no. 4 (Autumn 2007), pp. 29–43, and "'A Cooperative Strategy for 21st Century Seapower': A View from Outside," vol. 61, no. 2 (Spring 2008), pp. 25–38; Steve Carmel, "Commercial Shipping and the Maritime Strategy," vol. 61, no. 2 (Spring 2008), pp. 39–46; Gen. Victor E. Renuart, Jr., USAF, and Capt. Dane S. Egli, USCG, "Closing the Capability Gap: Developing New Solutions to Counter Maritime Threats," vol. 61, no. 2 (Spring 2008), pp. 15–24; Scott C. Truver, "Mines and Underwater IEDs in U.S. Ports and Waterways: Context, Threats, Challenges, and Solutions," vol. 61, no. 1 (Winter 2008), pp. 106–27; and Martin N. Murphy, "Suppression of Piracy and Maritime Terrorism: A Suitable Role for a Navy?" vol. 60, no. 3 (Summer 2007), pp. 23–45: all *Naval War College Review.*

12. Some examples include Jay Carafano and Martin Edwin Andersen, *Trade Security at Sea: Setting National Priorities for Safeguarding America's Economic Lifeline,* Backgrounder 1930 (Washington, D.C.: Heritage Foundation, 27 April 2006), available at www.heritage.org/; Michael D. Greenberg et al., *Maritime Terrorism: Risk and Liability* (Santa Monica, Calif.: RAND, 16 October 2006), available at www.rand.org/pubs/; and *Maritime Security* (Arlington, Va.: Lexington Institute, January 2008), lexingtoninstitute.org/docs/796.pdf. In addition, GlobalSecurity.org devotes a well informed page to MDA, www.globalsecurity.org/intell/systems/mda.htm.

13. *National Strategy for Maritime Security,* p. 1.

14. Data fusion, properly, is the process of combining data or information to determine what significant knowledge is present. See David L. Hall and James Llinas, *Handbook on Multisensor Data Fusion* (Boca Raton, Fla.: CRC, 2001).

15. See Pranab Dhal Samanta et al., "Lashkar Came via Sea from Karachi, Used Gujarat Boat to Reach Mumbai," Indian Express.com, 28 November 2008, www.indianexpress.com/; "Terrorists May Have Hijacked Porbander Fishing Boat," *Times of India,* available at timesofindia.indiatimes.com.

16. The FOSIFs and FOSICs were in Norfolk, London, Pearl Harbor, Rota (Spain), and Kamiseya (Japan). For detailed review of how operational intelligence supported Navy operations, see Christopher A. Ford, David A. Rosenberg, and Randy Carol Balano, *The Admirals' Advantage: U.S. Navy Operational Intelligence in World War II and the Cold War* (Annapolis, Md.: Naval Institute Press, 2005).

17. See Robert C. Rubel, "The Navy's Changing Force Paradigm," *Naval War College Review* 62, no. 2 (Spring 2009), pp. 13–24.

18. See "Maritime Headquarters with Maritime Operations Centers: An Enabling Concept for Maritime Command and Control," available at *Naval Supply Systems Command,* www.navsup.navy.mil/, p. 8.

19. U.S. Homeland Security Dept., *The National Plan to Achieve Maritime Domain Awareness,* p. ii [emphasis added].

20. U.S. Navy Dept., *Maritime Domain Awareness Concept* [Washington, D.C.: Navy Staff, 29 May 2007], available at www.navy.mil/navydata/cno/.

21. "International Convention for the Safety of Life at Sea (SOLAS), 1974 (with amendments)," chap. 5, available at www.imo.org/Conventions/. Warships are excluded.

22. AIS Live, for example, is a commercial website (www.aislive.com/trial.html) on which subscribers can see worldwide, AIS-derived vessel information.

23. John Morgan and Bud Wimmer, "Enhancing Awareness in the Maritime Domain," *CHIPS* (April–June 2005), available at www.chips.navy.mil/.

24. See the ICAO website, www.icao.int.